DETAILED ACTION

1. Pre-appeal conference was held on April 16, 2008 for pre-appeal brief filed on 03/06/2008. The examiner updated the search and called the applicant to include allowable features to independent claims and file a terminal disclaimer to disclaim USPN 7171539. Based on the interview, Examiner's amendment has been made for independent claims 1 and 13, and terminal disclaimer is filed and approved by the office.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John R. Lastova.

3. Claims 1 and 13 are amended as follows.

1 (Currently Amended) A data processing apparatus, comprising:

a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a ~~a~~ secure domain and a non-secure domain separated from the secure domain under hardware control, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being configured such that when executing a program in a secure

mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode;

a memory configured to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the memory containing a non-secure table and a secure table, the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor, and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor; ~~and~~

a memory management unit configured, upon receipt of a memory access request issued by the processor when access to an item; of data in the memory is required, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory, the memory management unit comprising an internal storage unit configured to store descriptors retrieved by the memory management unit from either the non-secure table or the secure table, and the internal storage unit comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table;

when the processor is operating in said at least one non-secure mode, the memory management unit being configured to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table, and when the processor is operating in said at least one secure mode, the memory management unit being configured to

perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the secure table, and

wherein the flag is used so that the internal storage unit does not need to be flushed every time the processor switches between said at least one secure mode and said at least one non-secure mode or vice versa.

13. (currently amended) A method of managing access to a memory in a data processing apparatus, the data processing apparatus comprising:

a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain separated from the secure domain under hardware control, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, the memory being configured to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the memory containing a non-secure table and a secure table, the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor, and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated

descriptor, the method comprising the steps of:

(i) issuing from the processor a memory access request when access to an item of data in the memory is required;

(ii) determining whether an internal storage of a memory management unit contains a required descriptor from which access control information can be derived to enable the memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request to the memory;

(iii) in the event that the required descriptor is not contained within the internal storage unit, retrieving from either the non-secure table or the secure table, depending on the mode of operation of the processor, the required descriptor, storing that required descriptor within the internal storage unit, and setting a flag to be associated with that required descriptor within the internal storage unit to identify whether that required descriptor is from said non-secure table or said secure table; and

(iv) using the access control information derived from the required descriptor to perform within the memory management unit one or more predetermined access control functions to control issuance of the memory access request to the memory;

such that when the processor is operating in said at least one non-secure mode, the memory management unit performs the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table, and when the processor is operating in said at least one secure mode, the memory management unit performs the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage

d

h d ever time the rocessor s witches between sa id at least one secure mode an said at least one non-secure mode or vice *versa,*

unit retrieved from the secure table~~(.)~~ ; and

wherein the flag is used so that the internal storage unit does not need to be flushed every time the processor switches between said at least one secure mode and said at lease one non-secure mode or vice versa.

Allowable Subject Matter

5. Claims 1-24 are allowed in light of pre-appeal conference and/or applied reference fails to discloses a secure domain and a non-secure domain separated from the secure domain under hardware control, a non secure table that is within the non-secure memory contains descriptors, and the internal storage unit comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table, wherein the flag is used so that the internal storage does not need to be flushed every time the processor switches between a secure mode and non-secure mode or vice versa, as recited in claims 1 and 13. Dependent claims are allowed based on dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136